



(19) RU<sup>(11)</sup> 2 163 745<sup>(13)</sup> С2  
(51) МПК<sup>7</sup> Н 04 L 12/00, G 06 F 13/00

РОССИЙСКОЕ АГЕНТСТВО  
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

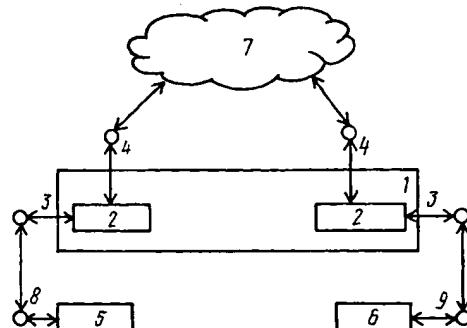
- (21), (22) Заявка: 99108495/09, 29.04.1999  
(24) Дата начала действия патента: 29.04.1999  
(46) Дата публикации: 27.02.2001  
(56) Ссылки: БРАНДМАКУЭРЫ INTERNET, ОБЗОР  
CW: Средства обеспечения безопасности в Internet, Computerworld, Россия, 27.08.1996,  
с.21-24. RU 2126170 С1, 10.02.1999. US  
5239648 A, 24.08.1993. US 4672533 A,  
09.06.1987. US 5018096 A, 21.05.1991. EP  
152900 A2, 28.08.1985. WO 94/06096 A2,  
17.03.1994. WO 93/21581 A2, 28.10.1993.  
(98) Адрес для переписки:  
197101, Санкт-Петербург, Большой просп.  
П.С., д.53, кв.14, Щеглову А.Ю.

- (71) Заявитель:  
Щеглов Андрей Юрьевич,  
Чистяков Антон Борисович,  
Клипач Виталий Степанович,  
Бутенко Валерий Владимирович,  
Джабаров Александр Артурович  
(72) Изобретатель: Щеглов А.Ю.,  
Чистяков А.Б., Клипач В.С., Бутенко  
В.В., Джабаров А.А.  
(73) Патентообладатель:  
Щеглов Андрей Юрьевич,  
Чистяков Антон Борисович,  
Клипач Виталий Степанович,  
Бутенко Валерий Владимирович,  
Джабаров Александр Артурович

(54) СИСТЕМА ЗАЩИТЫ ВИРТУАЛЬНОГО КАНАЛА КОРПОРАТИВНОЙ СЕТИ С АУТЕНТИФИЦИРУЮЩИМ  
МАРШРУТИЗАТОРОМ, ПОСТРОЕННОЙ НА КАНАЛАХ И СРЕДСТВАХ КОММУТАЦИИ СЕТИ СВЯЗИ  
ОБЩЕГО ПОЛЬЗОВАНИЯ

(57)  
Изобретение относится к вычислительной  
технике, а именно к информационным  
вычислительным системам, реализуемым на  
компьютерных сетях, и может быть  
использовано для защиты информационных  
ресурсов в корпоративных сетях. Технический  
результат состоит в повышении  
защищенности информационных ресурсов  
информационной вычислительной сети,  
повышении эффективности управления  
доступом к защищаемым ресурсам,  
реализации оперативного управления  
соединением по параметрам безопасности,  
фискальным контролем доступа к  
информации. Достигается это тем, что в  
систему защиты виртуального канала  
корпоративной сети, содержащую  
межсетевые экраны корпорации, введены  
защитные средства в клиентскую и серверную  
части, предназначенные для защиты ресурсов  
при взаимодействии клиент/сервис.  
Клиентская часть системы защиты состоит из  
блока приемо/передатчика, блока  
шифрования/расшифрования и электронной  
подписи, блока фильтрации служб по

стандартному протоколу, блока формирования  
закрытого протокола, блока стандартного  
сетевого оборудования клиента корпорации, а  
серверная часть состоит из блока  
приемо/передатчика, блока  
шифрования/расшифрования и электронной  
подписи, блока формирования служб по  
стандартному протоколу, блока формирования  
закрытого протокола, блока стандартного  
сетевого оборудования. 6 ил.



Фиг.1

R  
U  
2  
1  
6  
3  
7  
4  
5  
C  
2

R  
U  
1  
6  
3  
7  
4  
5  
C  
2



(19) RU (11) 2 163 745 (13) C2  
(51) Int. Cl. 7 H 04 L 12/00, G 06 F 13/00

RUSSIAN AGENCY  
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 99108495/09, 29.04.1999

(24) Effective date for property rights: 29.04.1999

(46) Date of publication: 27.02.2001

(98) Mail address:  
197101, Sankt-Peterburg, Bol'shoj prosp.  
P.S., d.53, kv.14, Shcheglov A.Ju.

(71) Applicant:  
Shcheglov Andrej Jur'evich,  
Chistjakov Anton Borisovich,  
Klipach Vitalij Stepanovich,  
Butenko Valerij Vladimirovich,  
Dzhabarov Aleksandr Arturovich

(72) Inventor: Shcheglov A.Ju.,  
Chistjakov A.B., Klipach V.S., Butenko  
V.V., Dzhabarov A.A.

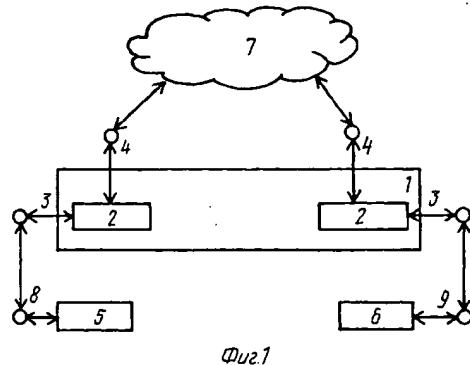
(73) Proprietor:  
Shcheglov Andrej Jur'evich,  
Chistjakov Anton Borisovich,  
Klipach Vitalij Stepanovich,  
Butenko Valerij Vladimirovich,  
Dzhabarov Aleksandr Arturovich

(54) PROTECTIVE SYSTEM FOR VIRTUAL CHANNEL OF CORPORATE NETWORK USING AUTHENTICATION  
ROUTER AND BUILT AROUND SHARED COMMUNICATION NETWORK CHANNELS AND SWITCHING  
FACILITIES

(57) Abstract:

FIELD: computer engineering; data computing systems using computer networks. SUBSTANCE: system that has L network-to-network corporate screens is provided, in addition, with protective facilities introduced in client's and server sections designed to protect resources during client/service interaction. Client's section has transceiver unit, encryption/decryption and electronic signature unit, service filtering unit using standard protocol, private protocol shaping unit, and standard network equipment unit of corporation client; server section has transceiver unit, encryption/decryption unit, service shaping unit using standard protocol, private protocol shaping unit, and standard network equipment unit. System provides for on-line control of connections according to safety

parameters and fiscal control of data access. EFFECT: improved protection of computer network data resources and their access control. 6 dwg



Dwg.1

R U  
2 1 6 3 7 4 5

C 2

R U  
2 1 6 3 7 4 5 C 2

R U 2 1 6 3 7 4 5 C 2

Изобретение относится к вычислительной технике, а именно к информационным вычислительным системам, реализуемым на компьютерных сетях, и может быть использовано для защиты информационных ресурсов в корпоративных сетях.

Известна система защиты ресурсов виртуального канала корпоративной сети, построенной на каналах и средствах коммутации сети связи общего пользования - межсетевой экран, например, CyberGuard (см. Computerworld, Россия, 27 августа 1996 года), Black Hole (Computerworld, Россия, 27 августа 1996 года). Она содержит выделенный компьютер, работающий под операционной системой Unix (например, UnixWare 2.1., FreeBSD) и функциональным программным обеспечением. Нет возможности контролировать и управлять соединением, используются данные служебных заголовков стандартных протоколов для получения аутентификационных признаков, администрирование достаточно негибко.

Наиболее близкой по технической сущности заявляемой (прототипом) является система защиты виртуального канала корпоративной сети, включающей в себя два или несколько межсетевых экранов. Система представлена на фиг. 1 в схеме защищенного взаимодействия клиент/сервер. Схема включает систему защиты 1, состоящую из M межсетевых экранов 2. Будем называть межсетевой экран, разграничающий подсеть с клиентами корпоративной сети и глобальную сеть, входным межсетевым экраном, а разграничающий подсеть с серверами корпоративной сети и глобальную сеть, выходным межсетевым экраном (разумеется, это сеансовые понятия). Вход/выход 3 входного межсетевого экрана 2 соединен с входом/выходом 8 клиентов корпорации 5, включающих в себя блок стандартной обработки запросов (стандартное сетевое ФПО), и является первым входом/выходом системы, вход/выход 3 выходного межсетевого экрана 2 соединен с входом/выходом 9 сервера корпорации 6 (стандартное сетевое ФПО) и является вторым входом/выходом системы. Вход/выход 4 входного межсетевого экрана соединен с каналом связи общей сети передачи данных 7, является третьим входом/выходом системы. Вход/выход 4 выходного межсетевого экрана соединен с каналом связи общей сети передачи данных и является четвертым входом/выходом системы.

Система защиты 1 состоит из M межсетевых экранов 2. Межсетевой экран 2 (см. фиг. 2) состоит из блока приемо/передатчика 10, блока фильтрации пакетов 11, блока шифрования/расшифрования и электронной подписи 12, блока аутентификации клиента по идентификатору, паролю и службе 13, блока регистрации 14, блока удаленного администрирования 15. Причем первый вход/выход системы защиты является входом/выходом 4 входного межсетевого экрана, второй вход/выход системы защиты является входом/выходом 4 выходного межсетевого экрана, третий вход/выход системы защиты является входом/выходом 3 выходного межсетевого экрана, четвертый вход/выход системы защиты является входом/выходом 3 выходного межсетевого

экрана; вход/выход 4 межсетевого экрана является первым входом/выходом блока приемо/передатчика 10, вход/выход межсетевого экрана 3 является третьим входом/выходом блока приемо/передатчика 10, второй вход/выход блока приемо/передатчика 10 соединен с первым входом/выходом блока фильтрации пакетов 11, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи 12, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по идентификатору, паролю и службе 13, второй вход/выход которого соединен с первым входом/выходом блока регистрации 14, второй вход/выход которого соединен с входом/выходом блока удаленного администрирования 15; первым входом/выходом межсетевого экрана является первый вход/выход блока приемо/передатчика 10, второй вход/выход межсетевого экрана является третьим входом/выходом блока приемо/передатчика 10.

Защищенное взаимодействие между клиентами и серверами корпорации осуществляется следующим образом. Рассмотрим взаимодействие в среде TCP/IP (может быть реализован и другой стек протоколов). Клиент 5 согласовывает свои права доступа с межсетевым экраном 2. С этой целью клиент 5 посыпает стандартный TCP/IP пакет, в котором содержится в заголовке IP-адрес клиента, IP-адрес сервера назначения и порт службы, в поле данных идентификатор клиента, пароль, в формате той службы, на порт которой посыпается пакет, причем поле данных может быть зашифровано секретным ключом межсетевого экрана, после этого, пройдя через блок приемо/передатчика 10, блок фильтрации пакетов 11, где происходит фильтрация пакетов по IP-адресу из служебного заголовка, блок шифрования/расшифрования и электронной подписи 12, где происходит расшифровка поля данных, если это необходимо, блок аутентификации клиента по идентификатору клиента, паролю и службе 13, где, зная службу из служебного заголовка пакета, происходит извлечение идентификатора клиента и пароля и поля данных стандартного пакета.

Далее происходит проверка по базе данных безопасности на существование клиента с данным идентификатором, на соответствие пароля идентификатору и определение соответствующего секретного ключа клиента и алгоритма защиты (шифрование/расшифрование, электронная подпись), и в случае удачного завершения проверки происходит пропуск пакета к серверу и установление соединения с клиентом, с поддержкой шифрования или электронной подписи с ключом, определенным для данного клиента, в случае неудачного результата проверки происходит разрыв соединения с предварительной отправкой сообщения клиенту о неудачно пройденной проверке и регистрацией в блоке регистрации. То же самое происходит и на межсетевом экране, отделяющем сервер корпорации от глобальной сети. После этого происходит защищенное взаимодействие по уже установленному соединению с поддержкой определенных (до установления соединения)

C 2  
5  
4  
5  
3  
7  
1  
6  
3  
C  
U

R  
U  
2  
1  
6  
3  
7  
4  
5  
C  
2

C  
2  
5  
4  
3  
7  
1  
6  
3  
C  
U

для данного клиента алгоритмов. Удаленное администрирование реализуется после установления защищенного взаимодействия как использование блока удаленного администрирования зарегистрированным в системе защиты пользователем.

Однако эта система защиты не обеспечивает полностью защищенное взаимодействие клиент/сервер. Это вызвано тем, что по существу при проверке используются служебные заголовки стандартных протоколов, которые могут быть подделаны (например, атака Митника), что облегчает несанкционированный доступ через межсетевой экран под видом стандартного клиента.

Также эта система подвержена стандартной атаке "Подмена маршрутизатора, используя управляющие протоколы" (например, Windows 95 - 1 раз в минуту производит автоматический поиск маршрутизатора. Windows NT - 1 раз в 10 минут по стандартному незащищенному протоколу).

Так как за каждым участником обмена закреплен свой IP-адрес, который используется и при маршрутизации и при аутентификации, невозможно скрытие топологии корпоративной сети и IP-адресов информационных серверов, что в принципе упрощает атаку на корпоративную сеть.

Поскольку после установления соединения клиент/сервер их взаимодействие осуществляется без участия системы защиты, отсутствует возможность отключения клиента даже в случае обнаружения его несанкционированных действий; например, средствами проверки целостности данных на сервере, не говоря уже о возможности контролирования взаимодействия клиент/сервер на всех стадиях.

Поскольку реализуется статичный способ управления доступом (посредством записи в базу данных доступных для клиента файлов и каталогов), доступ достаточно статичен, не позволяет быстро изменять настройки системы защиты, что оказывается на защищенности (реакция на атаку из-за ошибочной настройки медленная).

Поскольку в рассмотренной системе нет средств анализа зарегистрированных попыток неудачного доступа (обычно журналы регистрации проверяются людьми), реакция на попытки взлома может быть неадекватной и непредсказуемой (человеческий фактор).

Поскольку фиксируются только неудачные попытки, невозможно отследить сколько потеряно информации при использовании злоумышленниками идентификационных параметров действительного клиента.

Поскольку производится только фильтрация IP-адресов - происходит дополнительная проверка на аутентификационные признаки, например, в случае включения в корпоративную сеть SQL-сервера с собственной системой защиты.

Задача изобретения состоит в повышении защищенности информационных ресурсов информационной вычислительной сети, повышении эффективности управления доступом к защищаемым ресурсам, реализации оперативного управления соединением по параметрам безопасности, фискальном контроле доступа к информации.

Достиается это тем, что в систему защиты

виртуального канала корпоративной сети, содержащую  $n$  межсетевых экранов корпорации, каждый из которых состоит из блока приемо/передатчика, блока фильтрации пакетов, блока шифрования/расшифрования и электронной подписи, блока аутентификации клиента по идентификатору, паролю и службе, блока регистрации, блока удаленного администрирования, причем первый вход/выход межсетевого экрана является первым входом/выходом блока приемо/передатчика, второй вход/выход блока приемо/передатчика соединен с первым входом/выходом блока фильтрации пакетов, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи; первый вход/выход входного межсетевого экрана является первым входом/выходом системы защиты, дополнительно введены блок фильтрации служб по стандартному протоколу, блок формирования закрытого протокола, блок аутентификации клиента по IP-адресу, блок разрешения доступа по логическому имени сервера, блок выработки мандата на требуемые действия, блок проверки мандата клиента мандатом на требуемые действия, блок выработки маршрута, блок анализа журналов регистрации и блок оперативного управления.

Причем второй вход/выход блока шифрования/расшифрования и электронной подписи соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход блока фильтрации служб по стандартному протоколу соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по идентификатору, паролю и службе, второй вход/выход которого соединен с входом/выходом блока аутентификации клиента по IP-адресу, второй вход/выход которого соединен с входом/выходом блока проверки мандата клиента мандатом на требуемые действия, второй вход/выход которого соединен с входом/выходом блока разрешения доступа по логическому имени сервера, второй вход/выход которого соединен с входом/выходом блока выработки мандата на требуемые действия, второй вход/выход которого соединен с первым входом/выходом блока проверки мандата клиента мандатом на требуемые действия, второй вход/выход которого соединен с входом/выходом блока выработки маршрута, второй вход/выход которого соединен с первым входом/выходом блока регистрации, второй вход/выход которого соединен с первым входом/выходом блока анализа журналов регистрации, второй вход/выход которого соединен с входом/выходом блока оперативного управления, вход которого является вторым входом/выходом межсетевого экрана корпорации.

Кроме того, введена клиентская часть системы защиты, состоящая из блока приемо/передатчика, блока шифрования/расшифрования и электронной подписи, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока стандартного сетевого ФОП клиента корпорации, причем первый вход/выход блока приемо/передатчика

R U  
2 1 6 3 7 4 5 C 2

C 2  
5 4 3 7 1 6 C

является входом/выходом клиентской части системы защиты, второй вход/выход блока приемо/передатчика соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока стандартного сетевого оборудования клиента корпорации, вход/выход клиентской части системы защиты соединен с каналами и средствами коммутации сети связи общего пользования.

Кроме того, введена серверная часть системы защиты, состоящая из блока приемо/передатчика, блока шифрования/расшифрования и электронной подписи, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока стандартного сетевого ФПО сервера корпорации, причем первый вход/выход блока приемо/передатчика является первым входом/выходом серверной части системы защиты, второй вход/выход блока приемо/передатчика соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока стандартного сетевого ФПО сервера корпорации, вход/выход серверной части системы защиты соединен с каналами и средствами коммутации сети связи общего пользования.

На фиг.4 представлена схема защиты виртуального канала корпоративной сети с аутентифицирующим маршрутизатором, построенной на каналах и средствах коммутации сети связи общего пользования. Она содержит М межсетевых экранов, L клиентских частей системы защиты и N серверных частей защиты. Межсетевой экран состоит из блока приемо/передатчика, блока фильтрации пакетов, блока шифрования/расшифрования и электронной подписи, блока аутентификации клиента по идентификатору, паролю и службе, блока регистрации, блока удаленного администрирования, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока аутентификации клиента по IP-адресу, блока разрешения доступа по логическому имени сервера, блока выработки мандата на требуемые действия, блока проверки мандата клиента мандатом на требуемые действия, блока анализа журналов регистрации, блока выработки маршрута и блока оперативного управления.

Первый вход/выход блока приемо/передатчика является входом/выходом межсетевого экрана, второй вход/выход блока приемо/передатчика соединен с первым входом/выходом блока фильтрации пакетов, второй вход/выход которого соединен с первым входом/выходом

блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по идентификатору, паролю и службе, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по IP-адресу, второй вход/выход соединен с входом/выходом блока разрешения доступа по логическому имени сервера, второй вход/выход которого соединен с входом/выходом блока выработки мандата на требуемые действия, второй вход/выход которого соединен с первым входом/выходом блока проверки мандата клиента мандатом на требуемые действия, второй вход/выход которого соединен с входом/выходом блока выработки маршрута, второй вход/выход которого соединен с первым входом/выходом блока регистрации, второй вход/выход которого соединен с первым входом/выходом блока анализа журналов регистрации, второй вход/выход которого соединен с входом/выходом блока удаленного администрирования, вход которого соединен с выходом блока оперативного управления, вход которого является входом системы защиты, вход/выход межсетевого экрана является первым входом/выходом системы.

Клиентская часть системы защиты состоит из блока приемо/передатчика, блока шифрования/расшифрования и электронной подписи, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока стандартного сетевого ФПО клиента корпорации, причем вход/выход блока стандартного сетевого ФПО клиента корпорации соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом блока приемо/передатчика, второй вход/выход которого является входом/выходом клиентской части системы защиты.

Серверная часть системы защиты состоит из блока приемо/передатчика, блока шифрования/расшифрования и электронной подписи, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока стандартного сетевого ФПО сервера корпорации, причем вход/выход блока стандартного сетевого ФПО сервера корпорации соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом блока приемо/передатчика, второй вход/выход которого является входом/выходом клиентской

RU 1 6 3 7 4 5 C 2

части системы защиты; первым входом/выходом системы является первый вход/выход межсетевого экрана, вторым входом/выходом системы является вход/выход клиентской части системы защиты, третьим входом/выходом системы является вход/выход серверной части системы защиты.

Защищенная сеть содержит систему защиты информации в корпоративной сети 1. Система защиты состоит из М межсетевых экранов 2, L клиентских частей системы защиты 16 и N серверных частей защиты 17 (фиг.3). Межсетевой экран 2 состоит из блока приемо/передатчика 10, блока фильтрации пакетов 11, блока шифрования/расшифрования и электронной подписи 12, блока фильтрации служб по стандартному протоколу 19, блока формирования закрытого протокола 20, блока аутентификации клиента по идентификатору, паролю и службе 13, блока аутентификации клиента по IP-адресу 21, блока разрешения доступа по логическому имени сервера 22, блока выработки мандата на требуемые действия 23, блока проверки мандата клиента мандатом на требуемые действия 24, блока выработки маршрута 25, блока регистрации 14, блока анализа журналов регистрации 26, блока удаленного управления 15, блока оперативного управления 27.

Первый вход/выход блока приемо/передатчика 10 является входом/выходом межсетевого экрана 2, второй вход/выход блока приемо/передатчика 10 соединен с первым входом/выходом блока фильтрации пакетов 11, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи 12, второй вход/выход которого соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу 19, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола 20, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по идентификатору, паролю и службе 13, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по IP-адресу 21, второй вход/выход соединен с входом/выходом блока разрешения доступа по логическому имени сервера 22, второй вход/выход соединен с входом/выходом блока выработки мандата на требуемые действия 23, второй вход/выход соединен с первым входом/выходом блока проверки мандата клиента мандатом на требуемые действия 24, второй вход/выход которого соединен с первым входом/выходом блока выработки маршрута 25, второй вход/выход которого соединен с первым входом/выходом блока регистрации 14, второй вход/выход которого соединен с первым входом/выходом блока анализа журналов регистрации 26, второй вход/выход которого соединен с первым входом/выходом блока удаленного администрирования 15, вход которого соединен с выходом блока оперативного управления 27, вход которого является входом системы защиты 1, вход/выход межсетевого экрана 2 является первым входом/выходом системы 1.

Клиентская часть системы защиты 16 (фиг. 5) состоит из блока приемо/передатчика 10,

блока шифрования/расшифрования и электронной подписи 12, блока фильтрации служб по стандартному протоколу 19, блока формирования закрытого протокола 20, блока стандартного сетевого ФПО клиента 5 корпорации, причем вход/выход блока стандартного сетевого ФПО клиента 5 корпорации соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу 19, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола 20, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи 12, второй вход/выход которого соединен с первым входом/выходом блока приемо/передатчика 10, второй вход/выход которого является входом/выходом клиентской части системы защиты 16.

Серверная часть системы защиты 17 (фиг. 20) состоит из блока приемо/передатчика 10, блока шифрования/расшифрования и электронной подписи 12, блока фильтрации служб по стандартному протоколу 19, блока формирования закрытого протокола 20, блока стандартного сетевого ФПО сервера корпорации 6, причем вход/выход блока стандартного сетевого ФПО сервера корпорации 6 соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу 19, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола 20, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи 12, второй вход/выход которого соединен с первым входом/выходом блока приемо/передатчика 10, второй вход/выход которого является входом/выходом клиентской части системы защиты 16; первым входом/выходом системы 1 является первый вход/выход межсетевого экрана 2, вторым входом/выходом системы 1 является вход/выход клиентской части системы защиты 16, третьим входом/выходом системы 1 является вход/выход серверной части системы защиты 17.

Клиентская часть системы защиты, входящая в систему, может быть выполнена либо как ФПО на выделенном компьютере (см. Computerworld, Россия, 27 августа 1996 года), либо на выделенном процессоре или микроЭВМ, либо как часть комплекса ФПО на выделенном компьютере.

Серверная часть системы защиты может быть выполнена либо как ФПО на выделенном компьютере (см. Computerworld, Россия, 27 августа 1996 года), либо на выделенном процессоре или микроЭВМ, либо как часть комплекса ФПО на выделенном компьютере.

Дополнительно введенные в межсетевой экран блоки могут быть выполнены либо как ФПО на выделенном компьютере (см. Computerworld, Россия, 27 августа 1996 года), либо на выделенном процессоре или микроЭВМ, либо как часть комплекса ФПО на выделенном компьютере.

Система 1 в составе защищенной сети работает следующим образом.

Защищенное взаимодействие между клиентами и серверами корпорации осуществляется следующим образом.

R U  
2 1 6 3 7 4 5 C 2

R U  
1 6 3 7 4 5 C 2

Рассмотрим взаимодействие в среде TCP/IP (может быть реализован и другой стек протоколов). Клиент 5 согласовывает свои права доступа с межсетевым экраном 2. С этой целью на клиентской части 5 формируется стандартный TCP/IP пакет, в котором содержатся в заголовке IP-адрес клиента, IP-адрес сервера корпорации (который не обязательно должен существовать) и порт службы, в поле данных данные в формате той службы, на порт которой посыпается пакет, далее пакет попадает в блок фильтрации служб по стандартному протоколу 19. Если службы не имеют надежной защиты, далее пакет попадает в блок формирования закрытого протокола 20 и задерживается до получения ответа от межсетевого экрана 2 (в противном случае пропускается), в блоке 20 формируется пакет закрытого протокола, в котором содержится в заголовке служебный заголовок TCP/IP, но с IP-адресом межсетевого экрана 2 и портом установления соединения системы защиты 1, а в поле данных находятся поля идентификатора клиента, пароля, IP-адреса компьютера клиента, IP-адрес сервера назначения в зашифрованном виде.

Далее этот пакет попадает на межсетевой экран 2, где проходит проверки. Сначала проходит блок приемо/передатчика 10, далее блок фильтрации пакетов 11, где фильтруются служебные заголовки стандартных протоколов, далее блок шифрования/расшифрования и электронной подписи 12, где происходит расшифровка пакета, далее блок фильтрации служб по стандартному протоколу 19, где проверяется, нуждается ли данный пакет в аутентификации. Если нет, то он пропускается через блоки 12, 11, 10 к серверу, иначе пакет далее попадает в блок формирования закрытого протокола 20, где происходит разбор поля данных пришедшего пакета, далее в блок аутентификации клиента по идентификатору и паролю 13 (сравниваются присланные сведения и находящиеся в базе данных), далее в блок аутентификации клиента по IP-адресу 21 (сравниваются присланные сведения и находящиеся в базе данных), далее в блок разрешения доступа по логическому имени сервера 22 (сравниваются присланные сведения и находящиеся в базе данных), далее в блок выработки мандата на требуемые действия 23, далее в блок проверки мандата клиента мандатом на требуемые действия 24.

Далее, если все проверки пройдены и логический сервер относится к домену, обслуживаемому этим межсетевым экраном, то направляется пакет, разрешающий соединение между клиентом и межсетевым экраном (в противном случае пакет, инициирующий соединение, направляется дальше по IP-адресу серверу следующего ближайшего к требуемому серверу межсетевому экрану согласно маршруту, выработанному в блоке выработки маршрута 25), далее пакет, разрешающий соединение, состоящий из разрешающего флага и сеансового ключа. Пройдены проверки или не пройдены (отличие от прототипа, обслуживаемая блоком анализа журналов регистрации) попытка доступа фиксируется в журнале регистрации блоком регистрации 14 и далее обрабатывается соответственно настройкам блока анализа

журнала регистрации 26. Пакет, отправленный межсетевым экраном, приходит к клиенту, проходя блок приемо/передатчика и блок шифрования/расшифрования и электронной подписи попадает в блок формирования закрытого протокола 20, далее пропускается пакет, устанавливающий соединение по стандартному соединению, но в каждом пакете заменяются IP-адреса сервера назначения на IP-адрес межсетевого экрана. Причем, проходя через блок шифрования/расшифрования и электронной подписи, пакет обрабатывается алгоритмом шифрования, определенным для данного клиента, а в межсетевом экране расшифровывается, и в блоке формирования закрытого протокола меняется IP-адрес приемника на IP-адрес сервера назначения, определяемый по логическому идентификатору сервера, передаваемого в первом (инициализирующем) пакете.

Так как осуществляется маршрутизация по защищенному закрытому протоколу, то система защищена от атаки "Подмена маршрутизатора путем использования управляющих протоколов".

Так как используются регистрация всех попыток доступа и автоматический анализ их, возможно организовать фискальный доступ к информации, то есть фиксирование и отслеживание всех информационных потоков от отправителя к получателю, идентификационных параметров отправителя и получателя, что особенно важно при обслуживании учреждений, связанных с коммерческой, военной или государственной тайной.

Так как используется мандатный принцип, появляется альтернативный способ управления доступом, что позволяет путем гибких настроек с помощью статического метода управления (выделения области памяти методом разграничения прав) и динамического (мандатного) реализовать более эффективную по управлению виртуальную файловую систему. Например, выделение статически общей области памяти для чтения и внутри нее распределение по мандатам при наличии у каждого клиента своей статически прописанной области памяти.

Так как используется мандатный принцип, повышается защищенность объектов из-за того, что в явном виде прописываются права конфиденциальности (мандат) каждому субъекту, участвующему в доступе к ресурсам.

Так как используется закрытый протокол на этапе установления соединения, система более защищена, чем системы, использующие стандартные протоколы на этом этапе. Кроме того, предлагаемая система обладает достоинствами открытых систем, так как закрытый протокол используется только на этапе установления соединения, далее используются открытые протоколы и алгоритмы защиты (шифрования и электронной подписи).

Так как все пакеты проходят межсетевой экран (система не отключается в фазе передачи данных), появляется возможность управлять потоком на уровне виртуального канала (отключать при перегрузках или при получении оперативной информации о сворачивании атаки на информационные ресурсы от других средств защиты) на любом этапе

R U 2 1 6 3 7 4 5 C 2

этого взаимодействия посредством входа системы защиты через блок оперативного управления.

Так как используются система логических имен для серверов, а также динамическая трансляция адресов при проходе сквозь межсетевые экраны - достигается скрытие сетевых адресов (например, IP-адресов) как клиентских частей системы защиты, так и серверов корпоративной сети.

Так как все выходы в глобальную сеть из корпоративной сети при использовании данной системы защиты логически закрыты межсетевыми экранами (клиент не может обратиться к серверу напрямую, так как IP-адрес сервера неизвестен), рабочие станции и сервера корпорации находятся в подсетях корпоративной сети, где бы территориально они не находились.

Организовано управление на уровне виртуального канала. Если клиент обладает разрешением на администрирование межсетевого экрана, то, пройдя стандартную процедуру проверки, может удаленно администрировать межсетевой экран. Например, при сигнале об атаке с клиентского места или сервера (например, нарушение целостности на данных компьютерах) или перегрузках сети администратор безопасности может отключить соответствующих клиентов (подозрительных в первом случае и наименее приоритетных в другом) с межсетевого экрана данной корпорации.

При аутентификации расширяются параметры аутентификации - аутентификация проводится по идентификатору, паролю, службе, сетевому адресу, разрешению к требуемому серверу.

К достоинствам предлагаемой системы защиты можно отнести следующее:

1. Маршрутизация по защищенному закрытому протоколу.
2. Повышение производительности системы посредством отсутствия дополнительных аутентификационных проверок для хорошо защищенных служб.

3. Фискальный контроль доступа к информации и регистрация всех попыток доступа.

4. Мандатный принцип управления доступом для повышения эффективности управления доступом к ресурсам.

5. Закрытый протокол для логического выделения сети корпорации через средства

#### **6. Сокрытие сетевых адресов как клиента**

#### **7. Деление корпоративной сети с закрытым доступом на подсети**

## **8. Расширение функций аутентификации (по клиенту, по функциям, не по стандартному протоколом на подсети).**

9 Управление на уровне виртуального протокола

3. Управление на уровне виртуального канала (при перегрузках, при сигналах об атаке) через вход системы.

## Формула изобретения:

Система защиты виртуального канала корпоративной сети с аутентифицирующим маршрутизатором, построенная на каналах и средствах коммутации сети связи общего пользования, содержащая L межсетевых экранов корпорации, каждый из которых состоит из блока приемо/передатчика, блока фильтрации пакетов, блока шифрования/расшифрования и электронной

подписи, блока аутентификации клиента по идентификатору, паролю и службе, блока регистрации, блока удаленного администрирования, причем первый вход/выход межсетевого экрана является первым входом/выходом блока приемо/передатчика, второй вход/выход блока приемо/передатчика соединен с первым входом /выходом блока фильтрации пакетов, второй вход/выход которого соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, первый вход/выход указанного межсетевого экрана является первым входом/выходом системы, отличающейся тем, что в нее введены блок фильтрации служб по стандартному протоколу, блок формирования закрытого протокола, блок аутентификации клиента по адресу, блок разрешения доступа по логическому имени сервера, блок выработки мандата на требуемые действия, блок проверки мандата клиента мандатом на требуемые действия, блок выработки маршрута, блок анализа журналов регистрации и блок оперативного управления, причем второй вход/выход блока шифрования/расшифрования и электронной подписи соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока формирования закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока аутентификации клиента по индентификатору, паролю и службе, второй вход/выход которого соединен с входом/выходом блока аутентификации клиента по адресу, второй вход/выход которого соединен с входом/выходом блока разрешения доступа по логическому имени сервера, второй вход/выход которого соединен с входом/выходом блока выработки мандата на требуемые действия, второй вход/выход которого соединен с первым входом/выходом блока проверки мандата клиента мандатом на требуемые действия, второй вход/выход которого соединен с первым входом/выходом блока выработки маршрута, второй вход/выход которого соединен с первым входом/выходом блока регистраций, второй вход/выход которого соединен с входом/выходом блока удаленного администрирования, вход которого соединен с выходом блока оперативного управления, вход которого является вторым входом/выходом межсетевого экрана корпорации, введена клиентская часть системы, состоящая из блока приемо/передатчика, блока шифрования/расшифрования и электронной подписи, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока стандартного сетевого оборудования клиента корпорации, причем первый вход/выход блока приемо/передатчика является входом/выходом клиентской части системы, второй вход/выход блока приемо/передатчика соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом блока закрытого протокола, второй вход/выход

R U ~ 1 6 3 7 4 5 C 2

R U 2 1 6 3 7 4 5 C 2

которого соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока стандартного сетевого оборудования клиента корпорации, вход/выход клиентской части системы соединен с каналами и средствами коммутации сети связи общего пользования, введена серверная часть системы, состоящая из блока приемо/передатчика, блока шифрования/расшифрования и электронной подписи, блока фильтрации служб по стандартному протоколу, блока формирования закрытого протокола, блока стандартного сетевого оборудования сервера корпорации, причем первый вход/выход блока

приемо/передатчика является первым входом/выходом серверной части системы, второй вход/выход блока приемо/передатчика соединен с первым входом/выходом блока шифрования/расшифрования и электронной подписи, второй вход/выход которого соединен с первым входом/выходом закрытого протокола, второй вход/выход которого соединен с первым входом/выходом блока фильтрации служб по стандартному протоколу, второй вход/выход которого соединен с первым входом/выходом блока стандартного сетевого оборудования сервера корпорации, вход/выход серверной части системы соединен с каналами и средствами коммутации сети связи общего пользования.

15

20

25

30

35

40

45

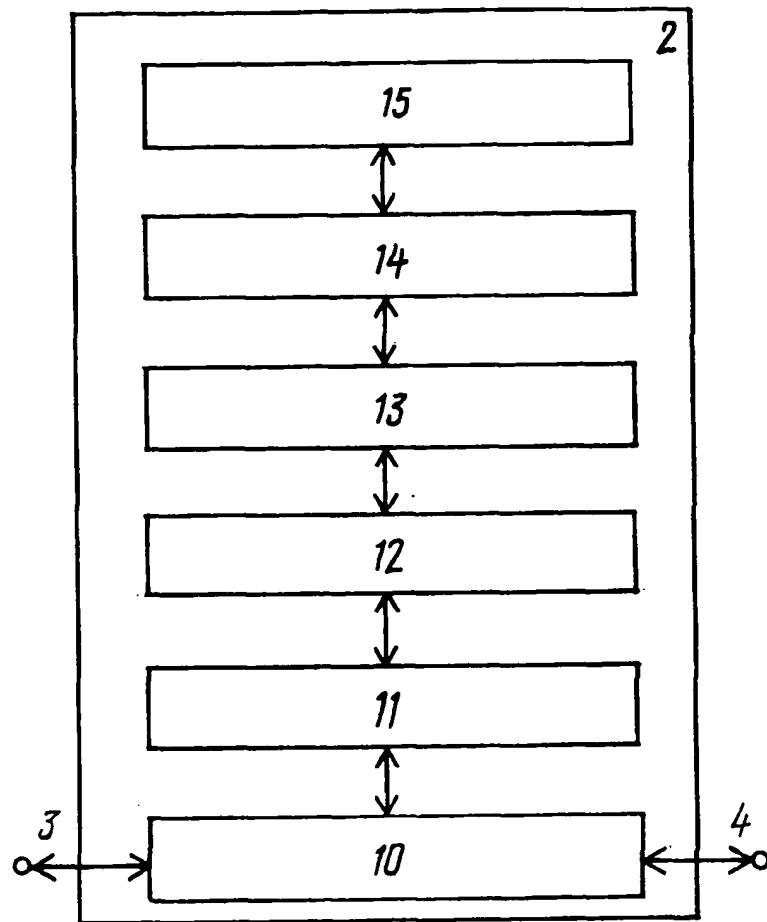
50

55

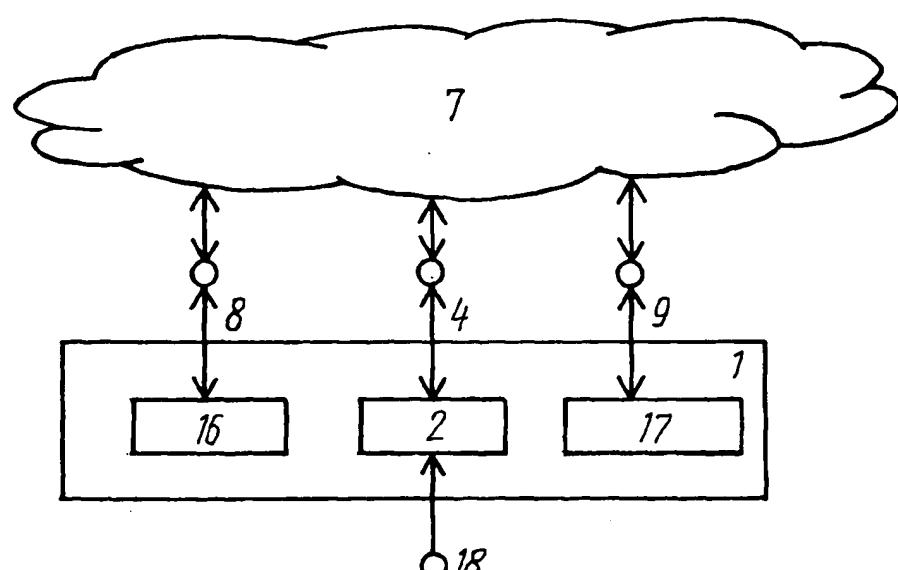
60

R U 2 1 6 3 7 4 5 C 2

R U 2 1 6 3 7 4 5 C 2



Фиг.2



Фиг.3

R U 2 1 6 3 7 4 5 C 2

R U ~ 1 6 3 7 4 5 C 2

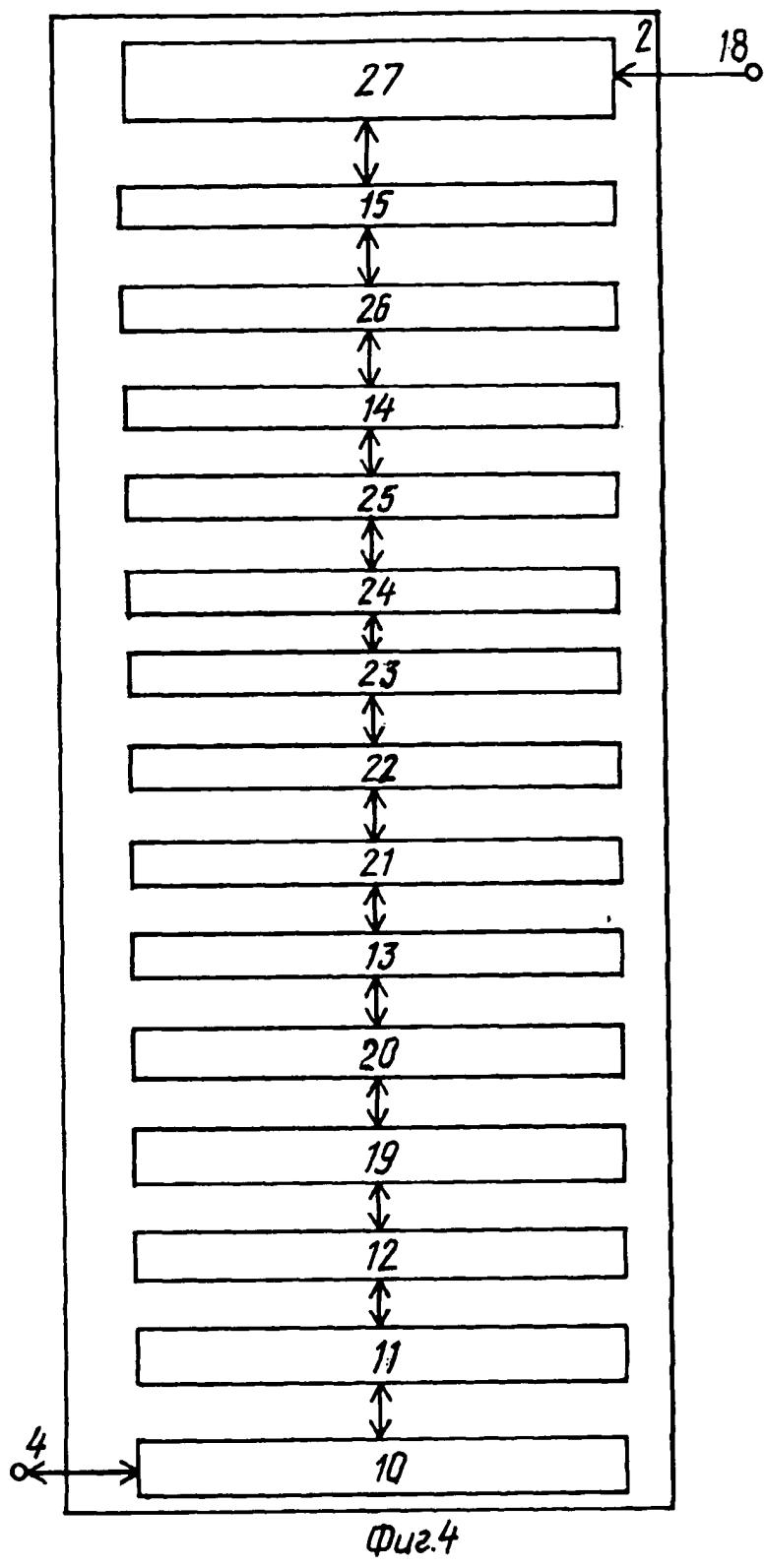
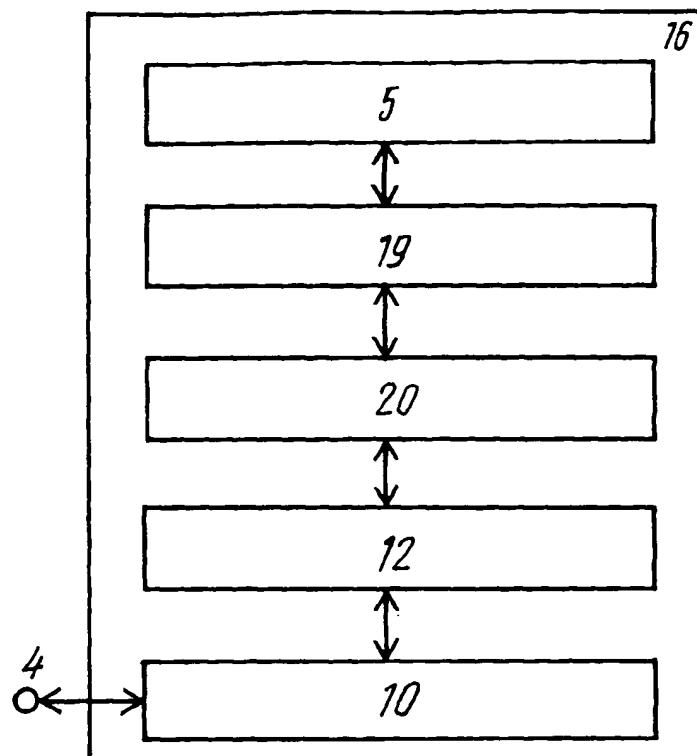


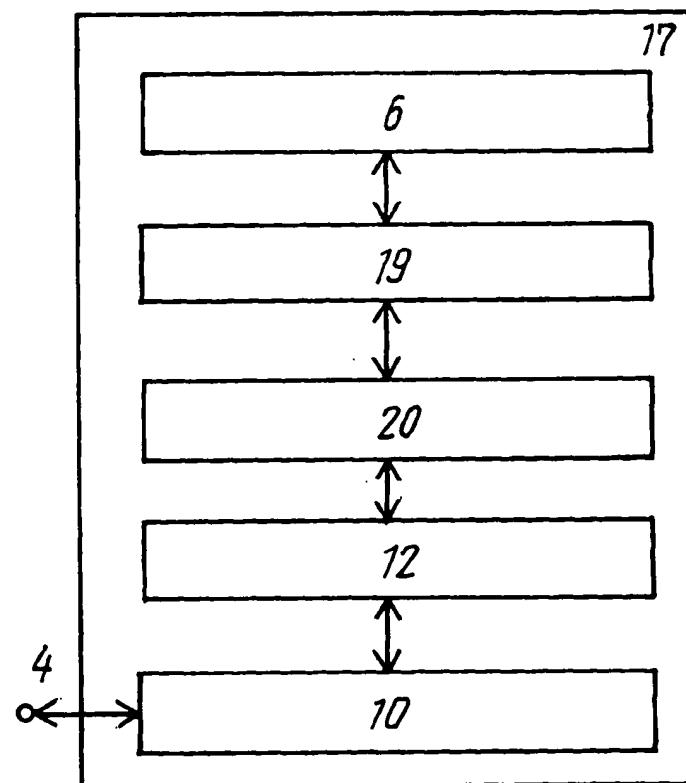
Fig.4

R U 2 1 6 3 7 4 5 C 2

R U 2 1 6 3 7 4 5 C 2



Фиг.5



Фиг.6

R U 2 1 6 3 7 4 5 C 2